## REMARKS

Claims 1-25 are pending in the present application. The Applicants respond to the issues identified in the Office Action mailed on April 30, 2007 as follows:

***Claim Rejections -- 35 USC § 112***

Claims 1-15 have been rejected under 35 U.S.C. 112, second paragraph, as being indefinite for not specifying when the "blocking access to the database for downloading the file" occurs. Applicants have amended claim 1 to specify that the blocking occurs "after the file has been downloaded or the period of time has expired." These limitations were previously included in claims 14 and 15, which have been cancelled.

***Claim Rejections -- 35 USC § 102***

Claims 1-4 and 14 have been rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Publication No. US 2003/0103615 to Baltes ("Baltes"). As noted above, the limitations in claims 14 and 15 have been incorporated into claim 1 and claims 14 and 15 have been cancelled.

Baltes discloses a method for automatically configuring a broadband communication device by downloading configuration information from a central server over a dial-up communications link. However, Baltes neither teaches nor suggests that once the configuration information is downloaded, subsequent access to this information is blocked so that an unauthorized user cannot gain access and download the information.

The Office Action states at page 4, line 22 to page 5, line 2 that:

> The Examiner also notes that access to the database for downloading the file is inherently blocked **eventually** after the file has been downloaded. (Emphasis added.)

The present invention is intended to limit access to files that are downloaded from a database over the Internet to provide security for the files. This is accomplished by limiting access to downloadable files to a predetermined period of time and blocking access after the file is downloaded or the period of time expires. Minimizing the window of time when a downloadable file can be accessed minimizes the risk of the file being downloaded by an unauthorized user.

The Examiner's use of the term "eventually" means that the database is accessible for an unknown and possibly extended period of time. Moreover, the finding that the "file is inherently blocked eventually" has no meaning because it is indefinite and speculative. "Eventually" could mean a week, a month, a year or several years. The Applicants' method provides security for downloadable files by allowing access to the files for a predetermined, finite period of time and immediately blocking access either after the file is downloaded or after the period of time expires in order to limit the possibility of access by unauthorized users. The method disclosed by Baltes does not limit when a file can be downloaded, nor does it block access to the file after the file is downloaded. Thus, the downloadable files in the method taught by Baltes can be downloaded numerous times over an indefinite period of time, without any protection from unauthorized users or hackers.

The Office Action states at page 5, lines 11-14 that:

> Baltes teaches the method of Claim 1, where the access to the database for downloading the file is inherently blocked after the file has been downloaded. **The Examiner interprets blocking access to the database as terminating the link between the database and the router.** (Emphasis added.)

There is no basis for finding that access to the downloadable file in Baltes is blocked after the file is downloaded. Baltes neither teaches nor suggests that access is blocked and the Examiner has not cited any reference that discloses such inherent blocking. Moreover, in many instances the file that is being downloaded is a generic file that is accessed and downloaded by multiple users. Therefore, such a file would not be blocked after it was downloaded. Accordingly, blocking access would not be "inherent."

Amended claim 1 states in relevant part that the method includes:

> permitting access to the database by the user for downloading the file for a period of time;
>
> downloading the file from the database to the managed device; and
>
> blocking access to the database for downloading the file <u>after the file has been downloaded or the period of time has expired</u>.

Amended claim 1 clearly teaches that, after the file has been downloaded from the database or after the period of time has expired, "access to the database for downloading the file" is blocked. Baltes neither teaches nor suggests that access to the database for downloading the file is blocked under any circumstances and the finding that access is "inherently blocked" is unsupported. Accordingly, the Applicants respectfully request that this finding be withdrawn.

The specification of the present application explains that the database is only available for downloading the file for a brief window of time or until the file has been downloaded. Thereafter, access to the file is blocked. The specification states at page 7, line 9 to page 8, line 2 that:

> Security is all about risk management and providing systems which minimize a computer network's exposure to risk. The present invention increases security, without the need to use any encryption mechanisms or devices that are hard to maintain, by reducing the time that the configuration file is available for downloading on the Internet. When a service provider makes configuration file (a file that contains configuration information for a particular program -- when the program is executed, it consults the configuration file to see what parameters are in effect) or other files available for downloading by a customer over the Internet, the file can be accessed by anyone who has the password and/or access code. This leaves an open door into the service provider's database and allows unauthorized hackers to downloading sensitive files. The method of the present invention opens the door only after the customer has signaled that it is ready to download the files and closes the door immediately after the downloading has been successfully, or in one embodiment unsuccessfully, completed. This allows hackers only a brief opportunity to gain unauthorized access to files in the service provider's database.

The Office Action states that: "The Examiner interprets blocking access to the database as terminating the link between the database and the router." In a very broad sense, this is correct, but it misinterprets claim 1. A dial-up communication link for accessing a database is substantially the same as communicating with a party over the telephone. If the telephone communication link is terminated (either by one party hanging up or an equipment malfunction), access between two parties ends and communication is at least temporarily blocked. However, in most cases, this does not prevent either party from dialing the other party's phone number, reestablishing the telephone communication link and continuing the conversation. Accordingly, the Examiner's interpretation of blocking access to the database as being equivalent to

terminating the link does not address the fact that access to the database can be just as easily "unblocked" by reestablishing "the link between the database and the router." Baltes does not address this issue, nor teach that access to the database is permanently blocked after a file is downloaded.

In the method disclosed by Baltes, configuration information is downloaded over a dial-up communication link and, when downloading is completed, the dial-up communication link is presumably terminated. This can only be presumed because Baltes does not disclose terminating the communication link. Moreover, Baltes does not disclose what would happen if the dial-up communication link was interrupted before the entire configuration file was downloaded. Baltes does not teach that the user would be prevented from reestablishing the dial-up communication link and downloading the configuration file for a second time. Moreover, there is no teaching or suggestion in Baltes that a hacker having the necessary information could not establish a dial-up communication link between the database and another router from a different location and illegally download the configuration file after the authorized user had already downloaded the file. Thus, Baltes does not provide security for the file because Baltes does not teach that access to the file in the database is restricted or blocked at any time.

Baltes teaches that the user is identified using "caller ID." However, this would not prevent a hacker from providing a false caller ID and accessing the database. An internet publication from the Commercial Law League of America (a copy is attached as Exhibit A of Applicants' January 29, 2007 Amendment) reports the first case brought by the FTC against a company for transmitting false caller ID data. Moreover, the internet website for the Attorney

General of Michigan (a copy is attached as Exhibit B of Applicants' January 29, 2007 Amendment --see page 2) reports that technology is available that allows thieves to choose the information they want to appear on caller ID. Therefore, the identification of the customer disclosed by Baltes (using caller ID, Smartcard or serial number) can be easily circumvented and, absent any teachings by Baltes to the contrary, a hacker could establish a dial-up communication link with the database and download a configuration file an unlimited number of times without any restrictions.

Accordingly, Baltes does not teach nor suggest "blocking access to the database for downloading the file" as required by claim 1 and the Applicants respectfully request that the Examiner withdraw the rejection of claims 1-4 as anticipated by Baltes.

***Claim Rejections -- 35 USC § 103***

Claims 6-8 and 15 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Baltes in view of an article titled, "A Temporal Authorization Model" by Bertino et al. ("Bertino"). Bertino discloses discretionary access to databases using authorizations that contain temporal information in order to control, "which users of the database may be granted authorizations to read and/or write data." See Introduction.

Bertino limits the validity of the authorization for accessing a database to temporal periods, but does not restrict or limit the availability of downloadable files on the database. Bertino neither teaches nor suggests limiting access to files to temporal periods and Bertino's method assumes that the files in the database are accessible at all times. Moreover, once an

authorization expires, there is nothing in Bertino's method that prevents an unauthorized user from accessing a file on the database using a different, "unexpired" authorization. In contrast, the Applicants' method limits when a file on a database is available for downloading to a predetermined window of time, regardless of the authorization for accessing the database. After this period of time expires, the window closes and the file is inaccessible to all authorization codes, no matter what their temporal periods of validity.

Bertino describes a method for database security which controls access to a system by providing users with authorizations that are limited to specified periods of time. "These assumptions allow us to consider the time *t* at which an access is requested and to look for a temporal authorization allowing that access at time *t*." See Bertino, 127, para. 2.1. After the period of time has elapsed, the user's authorization is invalid. In order to access the database, the user has to obtain another authorization, which is valid for a period of time. The temporal authorization method taught by Bertino only controls access to a database by limiting the period of time when a user's authorization is valid. Bertino does not limit access to files on the database to a period of time and, during any temporal period, numerous users with valid authorizations can access any file on the database. Once a user has gained access to the database, the method taught by Bertino does not prevent the user from accessing all of the files in the database.

The present invention does not limit the period of time when users can access a database but, instead, limits the period of time when individual files in the database can be accessed for downloading. Thus, users with a valid authorization for a temporal interval may not be able to

access files that are protected by the Applicants' method. The specification discloses at page 13, lines 1-5 that:

> Reducing the window of time that the ISP data center permits access to a configuration file for downloading significantly increases the security of files downloaded from the ISP's data center. In order to access the ISP data center and download files, a hacker has to know the serial number of a device and the password, as well as the date and time when the configuration file will be available for downloading by the customer.

In the temporal authorization method of Bertino, an unauthorized user must know the period of time when the authorization code allows access to a database. After an authorization code has expired, the unauthorized user can still access the database by obtaining another authorization code that allows access for another period of time. In contrast, in the Applicants' method, an unauthorized user must not only obtain an authorization code but, in order to download a secure file, he must also know when the database will allow access to the file for downloading. Thus, the Bertino method provides security for the authorization code for accessing a database, while the present invention provides security for individual files on the database. The advantage of the Applicants' method over the Bertino's method is that the Applicants' method has a predetermined, limited period of time during which downloading of a file is possible. In the Bertino method, the file is always available for downloading and, once an unauthorized user gains access to the database, there is no file security and any file can be accessed and downloaded.

The Office Action states at page 7, lines 11-14 that:

> It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Baltes with the teachings of Bertino.
>
> The motivation to combine is that Bertino teaches a well known technique in access control which **teaches limiting authorization using temporal constraints**. (Emphasis added.)

Combining Baltes and Bertino does not make the claims obvious because the claims do not "limit authorization using temporal constraints" but, instead, limits access to an individual file to a predetermined period of time. There is a fundamental difference between "limiting authorization using temporal constraints" as taught by Bertino and limiting access to a file to a window of time as required by the claims. Bertino teaches limiting users' ability to access the database, while the claims limit the access to files in the database so that neither authorized nor unauthorized users can access the files after they are downloaded or after the predetermined period of time expires.

Combining the teachings of Baltes and Bertino does not provide security for individual files. After a Baltes/Bertino authorization expires, an unauthorized user can still download a file by obtaining another authorization that is valid for a temporal interval. Accordingly, the file is only protected from being downloaded using the expired authorization but it is not protected from being downloaded using other authorizations that have not expired. In the Applicant's method, once the file is downloaded or the predetermined period of time expires, the file is blocked until the data base manager resets the time period and makes it available for

downloading. Therefore, the Applicants' method provides increased security that is not found by combining Baltes and Bertino.

Baltes and Bertino do not render claims 6-8 and 15 (nor any of the other claims) obvious, since these references, either alone or together, do not teach nor suggest a method for downloading a file which restricts access to the file to a period of time and which blocks access to a file either after the period of time expires or the file is downloaded. The authorization method taught by Bertino only limits individual user's authorization to temporal periods and does not restrict access to files in the database in any way. Moreover, one of ordinary skill in the art would not find it obvious in view of Bertino to set a time interval in the server for downloading files since the method taught by Bertino concerns user authorization and not access to files after the database is accessed.

Accordingly, the Applicants submit that claims 6-8 and 15 are not obvious in view of a combination of Baltes and Bertino and respectfully request that the Examiner withdraw the rejection based on these references.

Claims 5, 9-13, 16-17 and 21-24 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Baltes in view of U.S. Publication No. US 2002/0179709 to Mehler ("Mehler"), which discloses a bar code and scanner, but does not disclose a time interval for accessing a file in a database or blocking access to the file after it is downloaded. Accordingly, the teachings in Mehler do not overcome the deficiencies in Baltes. The combination of Baltes and Mehler neither teaches nor suggests a method for setting a time interval for downloading a

file and then blocking access to the file either after the file is downloaded or after the time interval expires.

Claims 18-20 and 25 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Baltes in view of Mehler as applied to claim 16 above and further in view of Bertino. The Applicants respectfully disagree with the finding in the Office Action at page 14, lines 1-2 that, "All the limitations of Claim[s] 18-20 and 25 are anticipated in the rejection of claim 16, except that the period of time is predetermined." As discussed above, the combination of Baltes and Mehler does not teach an interval of time for accessing a file and then blocking access at the end of the interval or after the file is downloaded. The teachings in Mehler do not overcome the deficiencies in Baltes, either alone or in combination with Bertino.

The claims in the present application restrict access to the database to a period of time and require coordination between the database and the user device so that an individual file is accessible for only a finite period of time. Bertino neither teaches nor suggests restricting the availability of a file for downloading to a predetermined period of time. Instead, Bertino limits the authorization for individual users to a temporal interval, without placing any temporal restrictions on users' access to individual files. As such, the temporal interval in Bertino neither teaches nor suggests the predetermined period of time in the claims during which a file is available for downloading.

The Office Action states at page 14, lines 7-10 that:

> It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Baltes with the teachings of Bertino.
>
> The motivation to combine is that Bertino teaches a well known technique in access control which **teaches limiting authorization using temporal constraints**. (Emphasis added.)

The Applicants respectfully disagree with this finding. The Applicants' method does not merely limit a user's authorization to access the database to a temporal interval but instead, limits the time period during which a file in a database can be accessed by a user. In the prior art methods, the files on a database are typically available to users on a 24-hours a day, 7-days a week basis. Bertino restricts authorization to temporal intervals, but does not restrict access to individual files on the database once a user accesses the database, either legally or illegally. In contrast, the Applicants' method provides increased security by minimizing the window of time during which unauthorized users (i.e., hackers) can illegally access and download individual files. Bertino does not restrict access to the file, either temporally or in any other way. Moreover, there is no teaching nor suggestion in Bertino that access to the file is blocked at any time.

Bertino limits user authorizations to temporal intervals but does not limit the time when files are accessible. The expiration of Bertino's temporal authorization period does not block access to individual files and files can be accessed at any time (perhaps weeks or months) by a user (either authorized or unauthorized) with an authorization that is valid for a particular interval. Thus, the method taught by Bertino does not provide security for individual files. The

claims of the present invention refer to "blocking access to the database for downloading the file" (see claim 1). The Applicants method provides security for downloadable files by restricting access to individual files to a predetermined period of time (preferably less than a few hours) and then blocking access after the time period elapses or the file is downloaded. Therefore, the time intervals in Bertino and in claim 1 are clearly distinguishable and one of ordinary skill in the art would not find that Bertino's authorization method using temporal intervals teaches or suggests limiting access to individual files to limited time intervals and then blocking access to the file after the file has been downloaded or after the time interval expires.

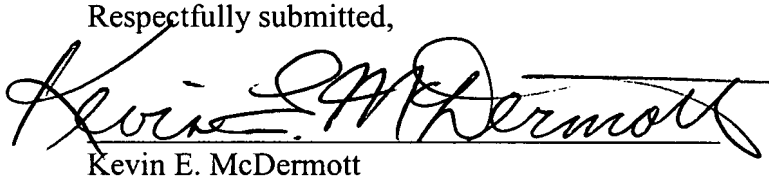
Accordingly, the Applicants submit that claims 18-20 and 25 are not obvious in view of Baltes, Mehler and Bertino, either alone or in combination, and respectfully request that the Examiner withdraw the rejection based on these references.

***Conclusion***

The Applicants submit that the arguments set forth above clearly distinguish the prior art references cited in the Office Action from the pending claims and, therefore, respectfully request early allowance of the claims.

If the Examiner has any questions or comments relating to the present application, he or she is respectfully invited to contact Applicants' attorney at the telephone number set forth below.

Respectfully submitted,



Kevin E. McDermott
Registration No.: 35,946
Attorney for Applicants

HOFFMANN & BARON, LLP
6900 Jericho Turnpike
Syosset, New York 11791
(516) 822-3550
KEM:___
271461_1